Hírlevél az ipari irányító rendszerek biztonságáról

A Black Cell elkötelezett az ipari irányító rendszerek (Industrial Control Systems – ICS), és/vagy kritikus infrastruktúrák biztonságának megteremtésében, ezért havonta hírlevelet bocsát ki a témában. A hírlevélben az érintett szervezetek, illetve kritikus infrastruktúra üzemeltetők tájékozódhatnak, valamint információkat nyerhetnek az ipari irányító rendszerek sérülékenységeiről; jó gyakorlatokról; a témát érintő képzésekről, oktatásokról, és konferenciákról; az ipari irányító rendszerek üzemeltetőit ért incidensekről. Az ipari irányító rendszerek biztonságáról szóló könyveket is ajánlunk, lehetőség szerint online elérhetőséggel. A Black Cell javaslatokat, megoldásokat kínál az ipari irányító rendszerekhez kapcsolódó tevékenységek hatékony elvégzéséhez, és ezáltal a biztonság minél magasabb szintű megteremtéséhez.

Tartalom:

ICS sérülékenységek

2019. októberben az alábbi ipari irányító rendszereket érintő sérülékenységeket publikálta a National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs), vagyis az ICS-CERT:

ICSA-19-302-01: **PHOENIX CONTACT Automation Worx Software Suite**
Magas szintű sérülékenység: Nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-302-01

ICSA-19-057-01: **Moxa IKS, EDS (Update A)**
Kritikus szintű sérülékenységek: Puffer túlcsordulás, CSRF, XXS, nem megfelelő hozzáférés ellenőrzés, túlzott hitelesítési kísérletek nem megfelelő korlátozása, érzékeny adatok hiányzó titkosítása, memória puffer határain kívüli olvasás lehetősége, hitelesítő adatok nem védett formában történő tárolása, kiszámítható műveletek, kontrollálatlan erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/ICSA-19-057-01

ICSMA-19-297-01: **Philips IntelliSpace Perinatal**
Közepes szintű sérülékenység: Erőforrás felfedése nem jogosultak számára.
https://www.us-cert.gov/ics/advisories/icsma-19-297-01

ICSA-19-297-01: **Rittal Chiller SK 3232-Series**
Kritikus szintű sérülékenységek: Kritikus funkcióban hiányzó autentikáció. Beégetett hitelesítő használat.
https://www.us-cert.gov/ics/advisories/icsa-19-297-01

ICSA-19-297-02: **Honeywell IP-AK2**
Közepes szintű sérülékenység: Kritikus funkcióban hiányzó autentikáció.
https://www.us-cert.gov/ics/advisories/icsa-19-297-02

ICSA-19-295-01: **Schneider Electric ProClima**
Kritikus szintű sérülékenységek: kód befecskendezés, a műveletek nem megfelelő korlátozása a memóriapufferben, keresési útvonal kontrollálatlansága.
https://www.us-cert.gov/ics/advisories/icsa-19-295-01

ICSA-19-290-01: **AVEVA Vijeo Citect and Citect SCADA**
Magas szintű sérülékenység: Puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-19-290-01

ICSA-19-290-02: **Horner Automation Cscape**
Magas szintű sérülékenységek: Nem megfelelő bemeneti hitelesítés, pufferen kívüli adat írás.
https://www.us-cert.gov/ics/advisories/icsa-19-290-02

ICSA-19-283-01: **Siemens Industrial Real-Time (IRT) Devices**
Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-283-01

ICSA-19-283-02: Siemens PROFINET Devices

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-283-02

ICSMA-19-274-01: Interpeak IPnet TCP/IP Stack (Update B)

Kritikus szintű sérülékenységek: puffer túlcsordulás, nem megfelelő érték kezelés, a műveletek nem megfelelő korlátozása a memóriapufferben, null pointer dereferencia, nem megfelelő argumentum kezelés a parancsban.
https://www.us-cert.gov/ics/advisories/icsma-19-274-01

ICSA-19-274-01: Interpeak IPnet TCP/IP Stack (Update A)

Kritikus szintű sérülékenységek: puffer túlcsordulás, nem megfelelő érték kezelés, a műveletek nem megfelelő korlátozása a memóriapufferben, null pointer dereferencia, nem megfelelő argumentum kezelés a parancsban.
https://www.us-cert.gov/ics/advisories/icsa-19-274-01

ICSA-19-192-02: Siemens SIMATIC WinCC and PCS7 (Update C)

Magas szintű sérülékenység: veszélyes fájltípus korlátozatlan feltöltési lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-192-02

ICSA-19-134-08: Siemens SIMATIC PCS7, WinCC, TIA Portal (Update D)

Kritikus szintű sérülékenységek: SQL befecskendezés, kivételek figyelmen kívül hagyása, interfész funkciók felfedése.
https://www.us-cert.gov/ics/advisories/ICSA-19-134-08

ICSMA-18-123-01: Philips Brilliance Computed Tomography (CT) System (Update A)

Magas szintű sérülékenységek: Szükségtelen privilegizált hozzáférés használat, forrás feltárás, beégetett hitelesítő használat.
https://www.us-cert.gov/ics/advisories/ICSMA-18-123-01

ICSA-16-313-02: Siemens Industrial Products Local Privilege Escalation Vulnerability (Update I)

Közepes szintű sérülékenységek: Nem megfelelő privilégium menedzsment.
https://www.us-cert.gov/ics/advisories/ICSA-16-313-02

ICSA-19-253-03: Siemens Industrial Products (Update A)

Magas szintű sérülékenységek: szoftver értékkezelési problémák (túlcsordulás), nem ellenőrzött erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-253-03

ICSA-19-281-01: SMA Solar Technology AG Sunny WebBox

Kritikus szintű sérülékenység: CSRF.
https://www.us-cert.gov/ics/advisories/icsa-19-281-01

ICSA-19-281-02: GE Mark VIe Controller

Közepes szintű sérülékenységek: Nem megfelelő hitelesítés, beégetett azonosítók használata.
https://www.us-cert.gov/ics/advisories/icsa-19-281-02

ICSA-19-281-03: Siemens SIMATIC WinAC RTX (F) 2010

Magas szintű sérülékenység: Nem ellenőrzött erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-281-03

ICSA-19-281-04: Siemens SIMATIC IT UADM

Közepes szintű sérülékenység: beégetett kriptográfiai kulcs használata.
https://www.us-cert.gov/ics/advisories/icsa-19-281-04

ICSMA-19-274-01: Interpeak IPnet TCP/IP Stack (Update A)

Kritikus szintű sérülékenységek: puffer túlcsordulás, nem megfelelő érték kezelés, a műveletek nem megfelelő korlátozása a memóriapufferben, null pointer dereferencia, nem megfelelő argumentum kezelés a parancsban.
https://www.us-cert.gov/ics/advisories/icsma-19-274-01

ICSA-19-274-01: Interpeak IPnet TCP/IP Stack

Kritikus szintű sérülékenységek: puffer túlcsordulás, nem megfelelő érték kezelés, a műveletek nem megfelelő korlátozása a memóriapufferben, null pointer dereferencia, nem megfelelő argumentum kezelés a parancsban.
https://www.us-cert.gov/ics/advisories/icsa-19-274-01

ICSA-19-274-02: Yokogawa Products

Magas szintű sérülékenység: Nem megfelelően jegyzett keresési útvonal vagy elem.
https://www.us-cert.gov/ics/advisories/icsa-19-274-02

ICSA-19-274-03: Moxa EDR 810 Series

Magas szintű sérülékenységek: nem megfelelő bemeneti hitelesítés, nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-19-274-03

A sérülékenységek részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://ics-cert.us-cert.gov/advisories

A sérülékenységek részletes leírását, a megoldási javaslatokat, és az érintett termékek teljeskörű listáját a sérülékenységhez tartozó linken lehet megtalálni.

ICS riasztások

2019. október hónapban az ICS-CERT nem adott ki riasztást.

A riasztások részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://www.us-cert.gov/ics/alerts

ICS jó gyakorlatok, javaslatok

Az ICS rendszerek elleni támadások száma évről évre növekvő tendenciát mutat. Sok kiberbiztonsági szakember szerint nem az a kérdés, hogy meg fog e történni egy kibertámadás valamely szervezet ellen, hanem az, hogy mikor.

A US. Department of Homeland Security, National Cybersecurity and Communications Integration Center egy 7 stratégiai lépésből álló védelmi megoldást kínál a következő linken elérhető dokumentumában:

https://www.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

1. Alkalmazás fehér lista alkalmazása
2. Biztosítsa a megfelelő konfigurációs beállításokat, és alkalmazzon patch menedzsmentet
3. Csökkentse a támadási felületet, például nem használt portok lezárásával
4. Megfelelő védelmi környezet kialakítása, megfelelően szegmentált hálózatok kialakítása
5. Megfelelő hitelesítés menedzsment kialakítása
6. Távoli hozzáférések biztonságossá tétele
7. Monitorozza a rendszer működését, és a megfelelő válaszreakciók kerüljenek alkalmazásra

A dokumentum részletezi a stratégiai lépések példákkal történő bemutatását.

ICS képzések, oktatások

A teljeség igénye nélkül 2019. novemberben ICS biztonság tárgyában a következő tréningek, oktatások kerülnek lebonyolításra:

2019. novemberben a következő tréning, oktatás kerül lebonyolításra az ICS/SCADA biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials SANS; Párizs, Franciaország; 2019. november 4-8.
- ICS410: ICS/SCADA Security Essentials SANS; Dubai, Egyesült Arab Emirátusok; 2019. november 24-28.

A részletek a következő webhelyen találhatók:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Időszakosan induló online kurzusok:

A https://www.coursera.org/ honlapon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során video oktatásokon vehet részt a jelentkező, és feladatok megoldásával demonstrálhatja tudását a szakterületet érintően. Az online tanfolyam elvégzését követően a Univesity of Colorado Boulder tanúsítványt állít ki a végzettek részére. A következő kurzusok végezhetők el:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

További részletek a következő webhelyen találhatók:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

Az említett oktatásokon felül az ICS-CERT is kínál Online kurzusokat:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity

További részletek a következő webhelyen találhatók:

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Az ICS-CERT Virtual Learning Portal (VLP) a következő képzések elvégzését teszi lehetővé:

- Operational Security (OPSEC) for Control Systems (100W) - 1 óra
- Differences in Deployments of ICS (210W-1) – 1.5 óra
- Influence of Common IT Components on ICS (210W-2) – 1.5 óra

- Common ICS Components (210W-3) – 1.5 óra
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 óra
- Cybersecurity Risk (210W-5) – 1.5 óra
- Current Trends (Threat) (210W-6) – 1.5 óra
- Current Trends (Vulnerabilities) (210W-7) – 1.5 óra
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 óra
- Attack Methodologies in IT & ICS (210W-9) – 1.5 óra
- Mapping IT Defense-in-Depth Security Solutions to ICS (210W-10) – 1.5 óra

Az ingyenes VLP képzések tapasztalatairól bővebb információ a Black Cell javaslatok részben található.

A részletek a VLP képzések ugyanazon a linken érhetők el, mint a többi ICS-CERT online kurzus.

A SANS nem kizárólag helyhez kötötten szervez képzéseket az ipari irányító rendszerek biztonságával kapcsolatban, hanem online kurzust is indít:

- ICS410: ICS/SCADA Security Essentials SANS

További részletek a következő webhelyen találhatók:

https://www.sans.org/find-training-beta/search?courses=2762&types=10&redirect=beta#__utma=195150004.1547647064.1563952209.1566466056.1568274011.4&__utmb=195150004.2.9.1568274014545&__utmc=195150004&__utmx=-&__utmz=195150004.1568274011.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=17428089

Az ipari irányító rendszerek és a SCADA rendszerek biztonságáról szóló Online kurzus érhető el az Udemy honlapján, ahol a jelentkező megtanulhatja az ICS/SCADA biztonság alapjait, technológiai megoldásokat, szoftver kezelést, szabályozási megoldásokat.

- ICS/SCADA Cyber Security

További részletek a következő webhelyen találhatók:

https://www.udemy.com/ics-scada-cyber-security/

A Department of Homeland Security 2 napos képzése során a résztvevők megismerhetik a különböző vezérlő rendszerek biztonságával kapcsolatos tudnivalókat.

- SCADA security training

További részletek a következő webhelyen találhatók:

https://www.tonex.com/training-courses/scada-security-training/

ICS konferenciák

A teljesség igénye nélkül a következő konferenciák kerülnek megrendezésre 2019. novemberben:

SCADA Security Conference

A nemzetközi konferencia témája a kritikus infrastruktúrák védelme, valamint az IoT (Internet of Things) eszközök védelme lesz. Az internetre csatlakoztatható eszközök között szerepelnek fizikai eszközök, járművek, otthoni háztartási eszközök és további beágyazott termékek, melyek rengeteg sérülékenységet tartalmaznak. Szó lesz továbbá a konferencián új ICS biztonsági trendekről, a témát érintő humán faktor jelentőségéről, okosvárosok biztonságáról, okosautók GDPR vonatkozásairól.

SCADA Security Conference; Prága, Csehország; 2019. november 4-5.

További részletek a következő webhelyen találhatók:

https://infosec-conferences.com/events-in-2019/scada-security-conference/
www.future-forces-forum.org/events/default/32_scada-security-conference?lang=en?ref=infosec-conferences.com

14th Annual API Cybersecurity Conference For The Oil & Natural Gas Industry

A 14. API kiberbiztonsági konferencia témája az energia védelme a kiberbiztonság megteremtésén keresztül. A Nozomi Networks szervezte konferencia az olaj és gáz ipar tekintetében a kiberbiztonság megvalósításának mikéntjét helyezi előtérbe, az elérhető biztonsági megoldások bemutatásán keresztül. A rendezvényen a téma szakértői a kihívásokat vitatják majd meg, illetve megosztják a megoldási javaslataikat.

14th Annual API Cybersecurity Conference For The Oil & Natural Gas Industry; Woodlands Texas, USA; 2019. november 12-14.

További részletek a következő webhelyen találhatók:

https://www.nozominetworks.com/upcoming-events/14th-annual-api-cybersecurity-conference-for-the-oil-natural-gas-industry/

Asia ICS Cyber Security Series

A 3. éves konferenciát egy kétnapos workshop előzi meg. A rendezvény a technikai és nem technikai beállítottságú személyeknek egyaránt megpróbál mély tudást adni a SCADA rendszerek kiberbiztonságáról. A következő iparágak lesznek a középpontban: víz és szennyvíz, energiatermelés és elosztás, olaj és gázipar, vegyipar, közösségi biztonság, közlekedés, okosvárosok, kommunikációs hálózatok.

Third annual ASIA ICS cyber security conference; Szingapúr, Szingapúr; 2019. november 25-26 és 27.

További részletek a következő webhelyen találhatók:

https://asiaicsc.com/

Digital Substations 2019

A 4. digitális alállomások éves konferenciája középpontjában egy rendszer megpályáztatásának és specifikációjának mikéntje, a tervezés és kivitelezés, a tesztelés és tanúsítás, valamint a működés és karbantartás áll, továbbá a jövőbeli rendszer fejlődése az IoT, a felhő technológiák és a gépi tanulás által.

Digital Substations 2019; Berlin, Németország; 2019. október 26-28.

További részletek a következő webhelyen találhatók:

https://www.smartgrid-forums.com/forums/digital-substations/?gclid=EAIaIQobChMIh_rYn9us5QIVyJQYCh3WfQlEEAAYBCAAEgLEPfD_BwE

ICS incidensek

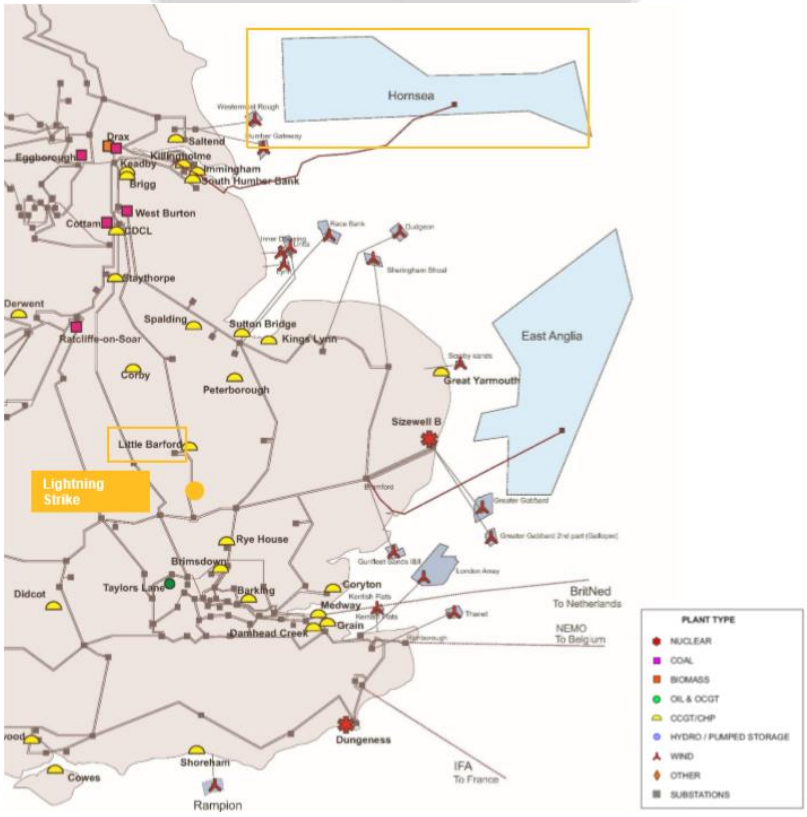
Nagy-Britanniai villamosenergia-rendszer kiesés

2019. augusztus 9-én a kelet-angliai áramellátó rendszert olyan incidens érte, amilyen nem volt már több, mint egy évtizede az országban. Erős esőzés, és szeles időjárás volt, valamint villámlott. Ez nem szokatlan ebben az évszakban Angliában, ezért is váratlanok voltak a következmények.

Egy villámcsapás érintette az átviteli rendszert, de ezt kezelte 0,1 másodperc alatt a védelmi rendszer. 20 másodperc alatt a normál működésre állt vissza a rendszer. Azonban közvetlenül a villámcsapás után másodperceken belül egymástól függetlenül a Hornsea szélerőmű és a Little Badford (gáz) erőmű csökkentette az energia betáplálását a hálózatba. A váratlan energia ellátási probléma a frekvencia rendkívüli gyorsasággal történő csökkenését eredményezte, és így a normál tartományból az kiesett 48,8 Hz-re (normál tartomány: 50.5Hz – 49.5Hz).

Az automatikus rendszer a tartalék energia forrása ellenére a legnagyobb hálózati generátor kiesését nem fedezte, annak ellenére, hogy a biztonsági és minőségi ellátási standard (SQSS) szerint működött a rendszer. Ebben az esetben szabályozott módon, az elosztási hálózat üzemeltetői által előre beállított paraméterekkel automatikusan leválasztja az ügyfeleket az ellátási hálózatról. Jelen esetben 5% ki lett kapcsolva az ellátásban a maradék 95% biztonsága érdekében.

A kiesés 1,1 millió ügyfelet érintett, ahol majd egy órán át teljesen kiesett az áramellátás. Ez több kritikus infrastruktúrát érintett az egészségügy és a közlekedés ágazatokban. A fővárosban, Londonban a vonatközlekedésben, a Newcastle-i repülőtéren, és az Ipswich-i kórházban okozott fennakadásokat a villamosenergia kiesése.



Az incidensről készült riport másodperc pontossággal, időrendben részletezi az eseményeket.

A riport szerint minden cselekmény a standardok szerint történt, a rendszerek beállításaitól az incidens kezelésig, ezért az esemény további elemzése vált szükségessé üzemeltetői és szabályozó oldalról egyaránt.

A riport további érdekes részletekkel a következő linken érhető el:

https://www.ofgem.gov.uk/system/files/docs/2019/08/incident_report_lfdd_-_summary_-_final.pdf

Szerző: 2 dolgot tartok fontosnak megemlíteni az incidens kapcsán. Az első az, hogy akkor is bekövetkezhet egy incidens, ha az üzemeltető mindenben megfelel a kötelezően betartandó jogszabályi előírásnak és a standardoknak, illetve a „best partice”-eket alkalmazza, és az ajánlásokban foglaltakat megfelelően implementálja. Ez a tevékenység végzésében benne lévő kockázat.

A másik, amely a riport olvasása során azonnal szemet szúrt, hogy a riport dokumentációs klasszifikációja HIGHLY CONFIDENTAL!!! Ennek ellenére nyíltan publikálásra került az interneten, és bárki által letölthető.

Könyvajánló

Az ipari irányító rendszerek összetett biztonságának elérése céljából került kiadásra a „Formális módszerek az ipari irányító rendszerek részére” című könyv.

A formális módszerek alatt azon metodológiákat kell érteni, amelyek a tervezési folyamattól kezdve matematikai elemzéssel alátámasztva próbálják leírni a rendszerek működését.

A könyv tartalmaz jó gyakorlatokat, esettanulmányokat arra vonatkozóan, hogy a magas integritási szintű rendszerek fejlesztése miként kell, hogy megvalósuljon. Tartalmazza a könyv továbbá a rendszerek különböző alkalmazásainak problémáit, illetve a problémák megoldására ajánlásokat.

A kommunikációs protokollok ellenőrzési módszereit is bemutatja a könyv, valamint felhasználó központú modellezés is bemutatásra kerül az együttműködés elemzése mellett.

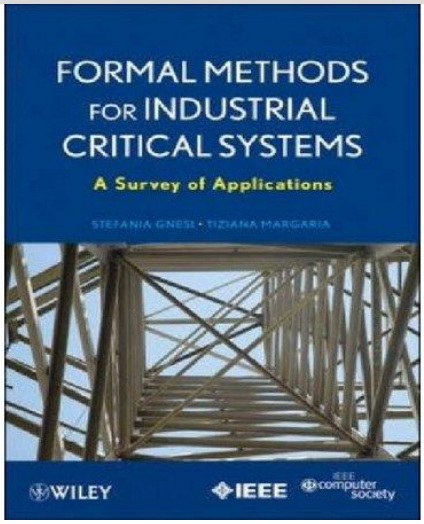
A könyv címe: **Formal Methods for Industrial Critical Systems: A Survey of Applications**

Szerzők: Stefania Gnesi, Tiziana Margaria

Kiadás éve: 2013.

A kiadvány elérhető a következő linken:

https://ieeexplore.ieee.org/book/6381798



Black Cell javaslatok

A Black Cell ipari irányító rendszerek biztonságáról kiadott hírleveleiben az első kiadástól kezdve ajánl bizonyos online és jelenlétet megkövetelő képzéseket.

A US. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) által kínált online oktatások ingyenesen elvégezhetők, és segítenek elsajátítani az ipari irányító rendszerek kiberbiztonsági sajátosságait. Regisztrációt követően el is lehet kezdeni a képzések elvégzését.

A következő képzések tapasztalatai kerülnek megosztásra jelen hírlevélben:

- Differences in Deployments of Industrial Control Systems

Az online képzés a International Association for Continuing Education and Training (IACET) által tanúsított, a kurzus végeztével tanúsítvány kerül kiállításra annak részére, aki elvégezte sikeresen a körülbelül 2 órás online tanfolyamot, és a 20 kérdésből álló teszten minimum 80%-ot elér.

A képzés során videók és egyéb látványos elemekkel tarkított megoldások segítségével lehet elsajátítani az ipari irányító rendszerekkel kapcsolatos alapfogalmakon túl az egyéb kritikus infrastruktúra elemekkel történő kapcsolatrendszer összefüggéseit.

A képzés során bizonyos témakörök lezárásaként a témakört érintő kérdésekre kell válaszolni, és kizárólag a helyes megoldás után engedi tovább folytatni a képzést a rendszer.

Példákon keresztül ismerheti meg a képzést végző személy az ICS rendszerek kiberbiztonságának jelentőségét. Az ICS rendszerek működésének folyamatai is bemutatásra kerülnek, amelyek segítik megérteni a működést, és az összefüggéseket.

- Cybersecurity Practices for Industrial Control Systems

2 képzés van jelenleg, amely akkreditált az IACET által, ez a másik. Ugyanúgy 80%-os vizsga esetén kap a résztvevő tanúsítványt.

Ez a képzés is körülbelül 2 órát vesz igénybe.

A képzés során bemutatásra kerül, hogy a kritikus információkat miként kell azonosítani, a fenyegetéseket elemezni, melyek a kritikus információk kapcsán merülnek fel, a sérülékenységek azonosítása és elemzése, a kockázatok értékelése, és a megfelelő védelmi intézkedések alkalmazása. Mindezek példákon keresztül, jól érthető módon kerülnek szemléltetésre.

A képzés során bizonyos témakörök lezárásaként a témakört érintő kérdésekre kell válaszolni, és kizárólag a helyes megoldás után engedi tovább folytatni a képzést a rendszer.

Egy izgalmas játék is a képzés része, ahol kritikus információk megszerzése a cél. Adott időn belül social engineering és egyéb technikák segítségével kell megszerezni a kritikus információkat, amelyekkel egy támadó az ipari irányító rendszerek működését befolyásolhatja.

- 210W-09 Cybersecurity for Industrial Control Systems - Attack Methodologies in IT & ICS

A képzés végén nincs külön vizsga, és nem akkreditált a képzés az IACET által, ettől függetlenül az ICS-CERT tanúsítványt bocsát ki azok részére, akik sikeresen végig veszik a képzési anyagot.

A képzés során bizonyos témakörök lezárásaként a témakört érintő kérdésekre kell válaszolni, és kizárólag a helyes megoldás után engedi tovább folytatni a képzést a rendszer.

A képzés végigveszi egy támadás összetevőit és mechanizmusát, ICS példákon keresztül bemutatva. Egy kémiai labor ipari irányító rendszere meghekkelésének fizikai következményét is bemutatja egy videón a képzés. Egy Man-in-the-middle támadás következtében a HMI nem mutat változást a rendszerben, miközben a laborban szivárogni kezd valamely kémiai funkció felgyorsításával a reakció következtében valamely vegyület.

A képzés végigveszi, hogy miként lehet azonosítani a támadásokat, és milyen módszerrel és technikákkal, tool-okkal lehet kivédeni vagy megelőzni esetleg mérsékelni a támadások hatásait.

- 210W-10 Cybersecurity for Industrial Control Systems - Mapping IT Defense-In-Depth Security Solutions to ICS

Ez a képzés is ICS-CERT tanúsítvánnyal zárul sikeres elvégzése esetén. A képzés elvégzésének folyamata az előző képzéssel azonos.

A kiberbiztonság területén a mélységi védelmi megoldások alkalmazása elengedhetetlen annak érdekében, hogy a támadók dolgát megnehezítsük. A képzés rétegzett szintek szerint mutatja be azokat a megoldásokat, amelyek segítenek a megfelelő védelmi szint kialakításában.

A szoftver rétegtől a hálózati és fizikai rétegen át a teljes biztonságmenedzsment szintig bemutatja a védelmi rétegek biztonsági megoldásait a kurzus, az ICS rendszerek alapul vételével.

- 210W-05 Cybersecurity for Industrial Control Systems - Cybersecurity Risk

Ez a képzés is ICS-CERT tanúsítvánnyal zárul sikeres elvégzése esetén. A képzés elvégzésének folyamata az előző képzéssel azonos.

A képzés sorra veszi a klasszikus kockázat menedzsment lépéseket, melyeket az ipari irányító rendszerek példáin keresztül mutat be az oktatás.

Az alapfogalmak is tisztázásra kerülnek annak érdekében, hogy a képzésben résztvevő személy tisztában legyen a folyamatokkal.

- 210W-08 Cybersecurity for Industrial Control Systems - Determining the Impacts of a Cybersecurity Incident

Ez a képzés is ICS-CERT tanúsítvánnyal zárul sikeres elvégzése esetén. A képzés elvégzésének folyamata az előző képzéssel azonos.

A képzés bemutatja, hogy miként alakulhatnak ki krízis helyzetek a működésben és az emberi élet veszélyeztetésében. A képzés egy hatalmas igazsága az ipari irányító rendszerek vonatkozásában: „A nem helyes adat rosszabb, mint ha nincs adat.”

Egy 15 perces videó bemutatja a 2005. március 23-án Texas Cityben történt British Petroleum olajfinomítóban történt robbanásos katasztrófát, annak következményeit és hatásait, a katasztrófa kialakulásához vezető úton a hibák középpontba állításával. Számos tényező közrejátszott abban, hogy a katasztrófa megtörténhetett. A mai napig tanulságokkal szolgálhat az eset, illetve a kockázatelemzésekhez inputot biztosíthat.

Szerző: Összességében az ipari irányító rendszerek biztonságában dolgozó bármely személy részére hasznosak a képzések, javasolt azok elvégzése. A videókban lassan és érthetően beszélnek az oktatók, így aki ért angolul, annak nincs nehéz dolga a képzések elvégzése során.

Nagyon jó, hogy példákon keresztül lehet megérteni az ICS rendszerek működésének, és a kiber veszélyek minden egyes aspektusának a sajátosságait. Akik a jelen hírlevélben bemutatott képzések további részletei iránt érdeklődnek, „ICS hírlevél" tárgyú e-mailjeiket küldjék a cara (kukac) blackcell.hu e-mail címre.

A képzések a következő linken érhetők el:

https://ics-cert-training.inl.gov/learn

A jelen hírlevél által nem részletezett képzések tapasztalatai a következő hírlevelek egyikében kerülnek bemutatásra.